



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/822,212	03/30/2001	Brian E. Marchant	60296-300202	1096

25696 7590 04/23/2004

OPPENHEIMER WOLFF & DONNELLY
P. O. BOX 10356
PALO ALTO, CA 94303

EXAMINER

SONG, HOSUK

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 04/23/2004

3

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/822,212

Applicant(s)

MARCHANT, BRIAN E.

Examiner

Hosuk Song

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 March 2001.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 43-62 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 43-47, 51-54, 58 and 59 is/are rejected.
- 7) ☒ Claim(s) 48-50, 55-57, 60-62 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 2.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-42 has been cancelled by Preliminary Amendment.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 43-47,51-54,58-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tajima et al.(US 5,517,614) in view of Yorke-Smith (US 5,548,648).

Claims 43,44: Tajima's patent discloses a memory stores a plurality of encryption/decryption algorithms in (col.2,lines 47;col.3,lines 54-60). Tajima discloses controller for selecting at least one of plurality of encryption/decryption algorithms in (fig.2 and col.3,lines 54-60). Tajima does not specifically disclose a first controller operable to read and select a portion of racetrack array based upon an array starting point and to utilize selected portion of racetrack array in at least one of plurality of encryption/decryption algorithms. Yorke-Smith's patent discloses this limitation in (fig.2 ;col.3,lines25-67 and col.4,lines 1-14). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ a first controller operable to read and select a portion of racetrack array based upon an array starting point and to utilize selected portion of racetrack array in at least one of plurality of encryption/decryption algorithms as taught in Yorke-Smith with data encryption method disclosed in Tajima in order to utilize a preset starting address and reducing a portion of the

data and processing required by the control bytes during the ciphering/deciphering operations thus avoiding distribution of complete array of random data.

Claim 51: Tajima discloses first processor includes a first controller and a first encryptor/decryptor in (fig.2).

Claim 52: Tajima discloses second processor includes a second controller and a second encryptor/decryptor in (fig.2).

Claims 45-47: Yorke-Smith patent discloses racetrack array is used to determine how many bytes of data are to be encrypted in (col.3,lines 25-50). Motivation to use racetrack array is discussed in claim rejection 43 above. ORing operation is disclosed in (col.9,lines 33-39).

Claims 53,54: Tajima discloses receiving data to be encrypted in (fig.1). Tajima discloses encrypting the determined number of bytes using the first encryption algorithm to form a first encrypted data stream in (col.3,lines 54-60). Tajima discloses encrypting the first encrypted data stream using the second encryption algorithm in (col.4,lines 19-29). Tajima does not specifically disclose using a first portion of racetrack array to determine how many bytes of data are to be encrypted, first portion beginning at starting address. Yorke-Smith patent discloses racetrack array is used to determine how many bytes of data are to be encrypted in (col.3,lines 25-50). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ a first controller operable to read and select a portion of racetrack array based upon an array starting point and to utilize selected portion of racetrack array in at least one of plurality of encryption/decryption algorithms as taught in Yorke-Smith with data encryption method disclosed in Tajima in order to utilize a preset starting address and reducing a portion of the data and processing required by the control bytes during the ciphering/deciphering operations thus avoiding distribution of complete array of random data.

Claims 58: Tajima discloses receiving data to be encrypted in (fig.1). Tajima discloses encrypting the determined number of bytes using the first encryption algorithm to form a first encrypted data stream in (col.3,lines 54-60). Tajima discloses encrypting the first encrypted data stream using the second encryption algorithm in (col.4,lines 19-29). Tajima does not specifically disclose using a first portion of racetrack array to determine how many bytes of data are to be encrypted, first portion beginning at starting address. Yorke-Smith patent discloses racetrack array is used to determine how many bytes of data are to be encrypted in (col.3,lines 25-50). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ a first controller operable to read and select a portion of racetrack array based upon an array starting point and to utilize selected portion of racetrack array in at least one of plurality of encryption/decryption algorithms as taught in Yorke-Smith with data encryption method disclosed in Tajima in order to utilize a preset starting address and reducing a portion of the data and processing required by the control bytes during the ciphering/deciphering operations thus avoiding distribution of complete array of random data.

Claim 59: Yorke-Smith discloses memory comprises a racetrack array of random data in (fig.7 and col.3,lines 25-50). Motivation to use racetrack array is discussed in claim rejection 58 above.

Allowable Subject Matter

3. Claims 48-50,55-57,60-62 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Atalla (US 4,870,683).
- b. Bruce Schneier (Applied Cryptography)

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hosuk Song whose telephone number is 703-305-0042. The examiner can normally be reached on Tue-Fri from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


HS